



SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES

**Visual Cryptography Base Shuffling Method for
Securing Medical Images**

التشفير المرئي المعتمد على طريقة الخلط لتأمين الصور الطبية

**A Thesis Submitted In Partial Fulfillment of the Requirements of Master
Degree in Computer of science**

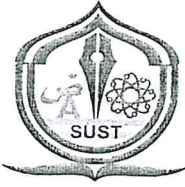
BY:

ALAA ALDEIN MOHAMED SULIMAN

SUPERVISOR :

DR. FAISAL MOHAMMED ABDALLA

February 2016



Approval Page

Name of Candidate: ALAA ALDEIN MOHAMED SULIMAN

Thesis title: Visual Cryptography Based On Shuffling
Method for Securing Medical Images

Approved by:

External Examiner

Name: Dr. Ali Ahmed Alaki Abdalla

Signature: [Signature] Date: 14/3/16

2. Internal Examiner

Name: Dr. Abuagla Babiker Mohammed Babiker

Signature: [Signature] Date: 5/3/2016

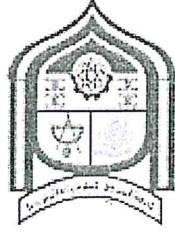
1. Supervisor

Name: Dr. Faisal Mohammed Abdalla Ali

Signature: [Signature] Date: 13-3-2016



Sudan University of Science and Technology
College of Graduate Studies



Declaration

I, the signing here-under, declare that I'm the sole author of the (M.Sc.) thesis entitled.....

..... Visual Cryptography Base Shuffling Method
..... For Securing Medical Images

which is an original intellectual work. Willingly, I assign the copy-right of this work to the College of Graduate Studies (CGS), Sudan University of Science & Technology (SUST). Accordingly, SUST has all the rights to publish this work for scientific purposes.

Candidate's name: Alaa Aldein Mohamed Suliman Ibrahim

Candidate's signature:  Date: 28.4.2016

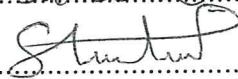
إقرار

..... أنا الموقع أدناه أقر بأنني المؤلف الوحيد لرسالة الماجستير المعنونة

..... التشفير المرئي المعتمد على طريقة الخلط
..... لتأمين الصور الطبية

وهي منتج فكري أصيل . وباختياري أعطى حقوق طبع ونشر هذا العمل لكلية الدراسات العليا - جامعة السودان للعلوم والتكنولوجيا، عليه يحق للجامعة نشر هذا العمل للأغراض العلمية .

اسم الدارس : علاء الدين محمد سليمان إبراهيم

توقيع الدارس :  التاريخ : 28/4/2016

الآية

قال تعالى: (قال النبي عليه علم من الكتاب أنا أتيتك به قبل أن يرتك إليكم
طرفي فلما رآه محتقرا عنه قال ههنا من فضل ربي ليبلونني أشكر أم
أكفر ومن شكر فأتما يحقر إنفحله ومن كفر فإن ربي غني كريم) صدق
الله العظيم حوراء النمل الآية 40 .

الحمد

الحمد لله رب العالمين والصلاة والسلام على سيدنا محمد بن عبدالله عليه أفضل الصلاة وأتم التسليم, الحمد لله الذي وفقني على إتمام هذا البحث فأحمدك حمداً أبلغ به رضاك وأودي به شكرك و أستوجب به المزيد من فضلك , اللهم لك الحمد كما أنت أهله ووليه.

DEDICATION

To the soul my father

To my dear beloved mother.

To my dear fellow brothers and sisters.

To all my friends and all those who have conferred their favors upon me
and paved my way to success.

To my teachers

ACKNOWLEDGEMENT

There is a list of people I would like to thank them. First of all would like to express enough thanks to my SUPERVISOR DR. FAISAL MOHAMMED ABDALLA for continued support. Besides my advisor, I would like thank Omran Ahmed Mohamed.

I would like to give special thanks and gratitude to the professors in the Faculty of Computer at SUDAN UNIVERSITY FOR SCIENCE AND TECHNOLOGY who were the best grow in our scientific career, for what they have offered to us from guidance and instruction patiently and modesty. The completion of this research could not have been possible without participation and assistance from Doctors and Master colleagues who considered as great addition to who I'm , so they deserve more than thanks specially MURTDA HASSEN and I'm very grateful to them.

Abstract

Visual Cryptography is a special encryption technique to encrypted visual information, which divides secret visual information into multiple layers Called shares, Each share holds some information. The receiver aligns the shares and the secret information is revealed by human vision without any complex computation .This thesis focuses on the visual cryptographic technique for encrypting of medical images before transmission or storage of them, This will make such images inaccessible by unauthorized personnel and also ensures confidentiality, The process made use of an encryption technique that is based on pixel shuffling and a secret key generated from the image, The algorithm is analyzed, based on the result of the analysis the difference between the plain image and the image rate was found after decoded is equal to zero.

المستخلص

التشفير المرئي هو إحدى التقنيات الخاصة بالتشفير والتي تستخدم في تشفير المعلومات المرئية (صور, نصوص, .. وغيرها) وذلك بتقسيم المعلومة المرئية السرية إلى طبقات متعددة تسمى بالأشهر كل شهر يحتوي على جزء من المعلومات المكونة للمعلومة المرئية الأصلية, مستلم الأشهر يقوم بطباعة تلك الأشهر على ورق شفاف ومحازاتها بطريقة محكمة عندئذ يمكن فك التشفير بواسطة عين الإنسان بدون أي حسابات معقدة, يركز هذا البحث على تقنية التشفير المرئية لتشفير الصور الطبية قبل نقلها أو تخزينها وهذا سيجعل من الصور لا يمكن الوصول إليه من قبل الأفراد غير المصرح لهم وكذلك يضمن السرية, النهج المستخدم في تقنية التشفير هذه هو خلط البكسل المكون للصورة باستخدام مفتاح تشفير تم توليده من الصورة, تم تحليل الخوارزمية وبناءً على نتيجة التحليل فقد وجدت معدل الإختلاف بين الصورة الأصلية و الصورة بعد فك شفرتها تساوي صفر.

TABLE OF CONTENTS

CHAPTER	TITEL	PAGE
	الأية	II
	الحمد	III
	DEDICATION	IV
	ACKNOWLEDGEMENT	V
	ABSTRACT	VI
	المستخلص	VII
	TABLE OF CONTENTS	VIII
	LIST OF TABLES	X
	LIST OF FIGURES	XI
1	INTRODUCTION	1
	1.1 Background	2
	1.2 Problem statement	4
	1.3 Research Objectives	4
	1.4 Important of Research:	4
	1.5 Research scope	5
	1.6 Research Methodology	5
	1.7 Research organization	6
2	LITERATURE REVIEW AND RELATED WORK	7
	2.1 Introduction	8
	2.1.1 Public and Private Key Encryption Systems	9
	2.1.2 Symmetric Encryption	9
	2.1.3 Asymmetric Encryption	10
	2.1.4 Monoalphabetic Substitution	12
	2.1.5 Polyalphabetic Substitution	12
	2.1.6 Transpositional Cipher	12
	2.1.7 Cryptographic goals	13
	2.2 Visual secret sharing scheme	14
	2.3 Black and White Visual Cryptography Schemes	14
	2.4 (2, 2) Visual Cryptography Scheme	15
	2.5 (k, n) Visual Cryptography Scheme	16
	2.6 Visual Cryptography Scheme for General Access Structure	17
	2.7 Visual Cryptography Scheme for Grey images	17

	2.8 Visual Cryptography Scheme for Color images	17
	2.9 Related Works	19
3	METHODOLOGY AND TOOLS	
	3.1 Overview	27
	3.2 Types of Digital image	27
	3.2.1 Binary images	27
	3.2.2 Grayscale image	27
	3.2.3 Color images	27
	3.3 Medical Image	28
	3.3.1 X Ray Image	28
	3.3.2 Magnetic resonance imaging (MRI)	28
	3.4 Proposed Method	28
	3.5 RGB colors shuffled Algorithm	31
	3.6 Application and tools	33
4	RESULTS AND DISCUSSION	34
	4.1 Results	35
	4.2 Discussion	45
	4.3 Statistical analysis	45
5	CONCLUSION AND RECOMMENDATION	47
	5.1 Conclusion	48
	5.2 Recommendation	48
	5.3 Future work	48
	Reference	49

LIST OF TABLES

TITEL	PAGE
Table2.1 : Naor and Shamir's scheme for encoding a binary pixel into two shares	15
Table 2:2 (2 out of 2) using 2 subpixels per original pixel	16
Table1 2.3: Related works comparison	25
Table 4.1: Entropy values of the plain image, cipher image and Reconstructed Image	36
Table 4.2: comparisons with existing techniques	36

LIST OF FIGURES

FIGURE NO	TITEL	PAGE
	Figure 2.1: The role of cryptography	9
	Figure 2.2: Symmetric Encryption	10
	Figure 2.3: Asymmetric Encryption	11
	Figure 2.4: The Caesar cipher	12
	Figure 2.5: Schematic diagram of SCOSVC algorithm (a) Encoding algorithm (b) Decoding algorithm	20
	Figure 2.6: Block diagram of the overall procedure	22
	Figure 2.7: The flow chart diagram for the encryption and decryption process	23
	Figure 2.8 Overall process of (VLKBVCSCI)	24
	Figure 3.1: The encryption and the decryption process	30
	Figure 3.2: Flow chart for RGB Pixel-Shuffling Encryption and create share using secret key	32
	Figure 4.1: Graphical user interface for encryption process	35
	Figure 4.2: Graphical user interface for decryption process	36
	Figure 4.3: Encryption Ultra sonic Image of the womb	37
	Figure 4.4: Decryption Ultra sonic Image of the womb	38
	Figure 4.5: Encryption X-ray picture of the brain	39
	Figure 4.6: Decryption X-ray picture of the brain	40
	Figure 4.7: Encryption X-ray picture of the brain	41
	Figure 4.8: Decryption X-ray picture of the brain	42
	Figure 4.9: Encryption X-ray picture of the ribs	43
	Figure 4.10: Decryption X-ray picture of the ribs	44

CHAPTER 1
INTRODUCTION

1.1 Background:

The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals [1].

Throughout history, however, there has been one central problem limiting widespread use of cryptography. That problem is key management. In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information. Consequently, the term key management refers to the secure administration of keys to provide them to users where and when they are required [1].

Historically, encryption systems used what is known as symmetric cryptography. Symmetric cryptography uses the same key for both encryption and decryption. Using symmetric cryptography, it is safe to send encrypted messages without fear of interception (because an interceptor is unlikely to be able to decipher the message); however, there always remains the difficult problem of how to securely transfer the key to the recipients of a message so that they can decrypt the message. A major advance in cryptography occurred with the invention of public-key cryptography. The primary feature of public-key cryptography is that it removes the need to use the same key for encryption and decryption. With public-key cryptography, keys come in pairs of matched “public” and “private” keys [1].

The public portion of the key pair can be distributed in a public manner without compromising the private portion, which must be kept secret by its owner. An operation (for example, encryption) done with the public key can only be undone with the corresponding private key [1].

The usage of the internet for the transmission of multimedia content has become a very frequent medium for the exchange of digital information almost all institutions that are using the internet. It is therefore important to secure data over open and unsecured networks in order to ensure safety of sensitive data. Medical information of patients are sensitive and needed to be protect during storage, and during transmission between two hospitals. When a physician receives a visit from a patient, he often requires a specialist opinion before giving a diagnosis. One possible solution is to send images of the patient, along with a specialist report, over a computer network. Nevertheless, computer networks are complex and espionage is a potential risk. We are therefore faced with a real security problem when sending data. For ethical reasons, medical imagery cannot be sent when such a risk is present, and has to be better protected hence the usage of cryptography in the protection of such data is very crucial.

The cryptography in digital computing has been applied to different kinds of digital file formats such as text, images video etc [2].One of the best-known techniques of visual cryptography has been credited to Moni Naor and Adi Shamir.

1.2 Problem statement:

The increased growth in the use of transmission of multimedia medical contents over unsecured and open networks provides insecurity for confidential patient information over these networks. Nowadays; modern Hospital Data Management Systems (HDMSs) are applied in a computer network; in addition medicinal equipments produce medical images in a digital form. HDMS must store and exchange these images in a secured environment to provide image integrity and patient privacy.

Digital encryption of medical images before transmission and storage is proposed as a way to effectively provide protection of patient information.

Is necessary in order to ensure inaccessibility of information to unauthorized personnel with patient

1.3 Research Objectives:

- 1 - To Provide protection of patient information.
- 2 - The medical image cannot be understood by anyone for whom it was unintended so as to achieve Confidentiality.
- 3 - The recipient must be able to determine if the medical image was altered during transmission to achieve integrity, if data integrity is preserved, the data can be considered consistent and can be given the assurance to be certified and reconciled.

1.4 Important Research:

Indeed, transferring or store medical data without applying security techniques means low level of privacy for patients protecting medical images from an unauthorized use is an essential requirement.

The most important security services required are patient privacy and medical image integrity, these challenges of confidentiality arising from the storage and transmission of medical data cannot be left to physicians alone.

These security services can be provided using Visual Cryptographic Encryption Technique.

1.5 Research scope:

Currently, most of Hospital Data Management Systems (HDMSs) and medical equipments are working in a computer network environment. Medical images are produced and stored in a digital form; moreover, they are exchanged through a computer network. These images are the most important entity in the healthcare diagnostic procedures because they are used to view features of patients such as anatomical cross-sections of internal organs and tissues, in addition they are used for physicians to evaluate the patient's diagnosis and monitor the effects of the treatment it is necessary to find an efficient way to transmit them over networks.

This thesis focuses on the visual cryptographic technique for encrypting of medical images before transmission or storage of them.

1.6 Research Methodology:

Two main methods are used for securing the images: changing the properties of the image itself, and encrypting the produced parts of the images during the processing using secret key.

Three major steps are used followed in changing the image properties : Extract the RGB components from the original image so as to produce three platters from that image, transpose(permute) the columns with rows for each platter , then reshaping the pixels for each platter.

Secret key is generated before the pre-mentioned three steps in the preceding paragraph. The key is used in two places: the first place is before producing the three platters in order to change the original format of the image. The second place is after the transposition step (the second step mentioned in the first paragraph); the key is used once again in order to change the format of that platter.

1.7 Research organization:

This Research has the following structure: Chapter 1 is Introduction, Chapter 2 is about Literature Review and related works, Chapter 3 explains the methodology employed for the encryption and the decryption process of the medical images and presents the mathematical algorithms employed to come out with a shares . Chapter 4 presents the results and discussion of the Shares obtained from the implementation of the algorithm used in the encryption process, and Chapter 5 concludes this work and explains the future directors.

CHAPTER 2

LITERATURE REVIEW AND RELATED WORK

2.1 Introduction:

Encryption is a modern form of cryptography that allows a user to hide information from others. Encryption uses a complex algorithm called a cipher in order to turn normalized data (plaintext) into a series of seemingly random characters (cipher text) that is unreadable by those without a special key in which to decrypt it. Those that possess the key can decrypt the data in order to view the plaintext again rather than the random character string of cipher text. Two of the most widely used encryption methods are Public key (asymmetric) encryption and Private key (symmetric) encryption. The two are similar in the sense that they both allow a user to encrypt data to hide it from others, and then decrypt it in order to access the original plaintext. They differ, however, in how they handle the steps between encryption and decryption [3].

The word cryptography has come from a Greek word, which means secret writing. In the present day context it refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. For private communication through public network, cryptography plays a very crucial role. The role of cryptography can be illustrated with the help a simple model of cryptography as shown in Fig.2.1. The message to be sent through an unreliable medium is known as plaintext, which is encrypted before sending over the medium. The encrypted message is known as ciphertext, which is received at the other end of the medium and decrypted to get back the original plaintext message

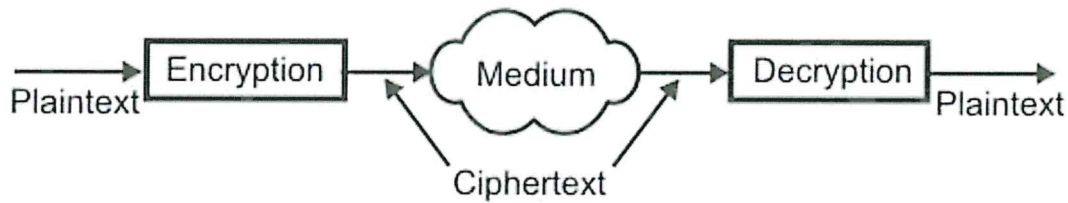


Figure 2.1: The role of cryptography

2.1.1 Public and Private Key Encryption Systems:

Private and public keys are used when creating digital signatures for authenticating the identity of an electronic document sender. These keys are used in two main encryption systems: Symmetric and Asymmetric.

2.1.2 Symmetric Encryption:

This system uses only private keys, which can be anything from a numerical symbol to a string of random letters. These private keys are used to encode a message, so that only the sender and the recipient of the message who know what the secret key is can “unlock” it and decrypt it. The system works pretty much like two best friends using a decoder ring to send secret messages to each other. The symmetric system’s only downside is the potentially unsafe private key transmission via the Internet, where other people can “crack” it and decode the message [3].

The cipher, an algorithm that is used for converting the plaintext to ciphertext, operates on a key, which is essentially a specially generated number (value). To decrypt a secret message (ciphertext) to get back the original message (plaintext), a decrypt algorithm uses a decrypt key. In symmetric key cryptography, same key is shared, i.e. the same key is used in both encryption and decryption as shown in Fig.2.2. The algorithm used to decrypt is just the inverse of the algorithm used for encryption. For example, if addition and

division is used for encryption, multiplication and subtraction are to be used for decryption.

Symmetric key cryptography algorithms are simple requiring lesser execution time. As a consequence, these are commonly used for long messages.

However, these algorithms suffer from the following limitations:

- Requirement of large number of unique keys.
- Distribution of keys among the users in a secured manner is difficult.

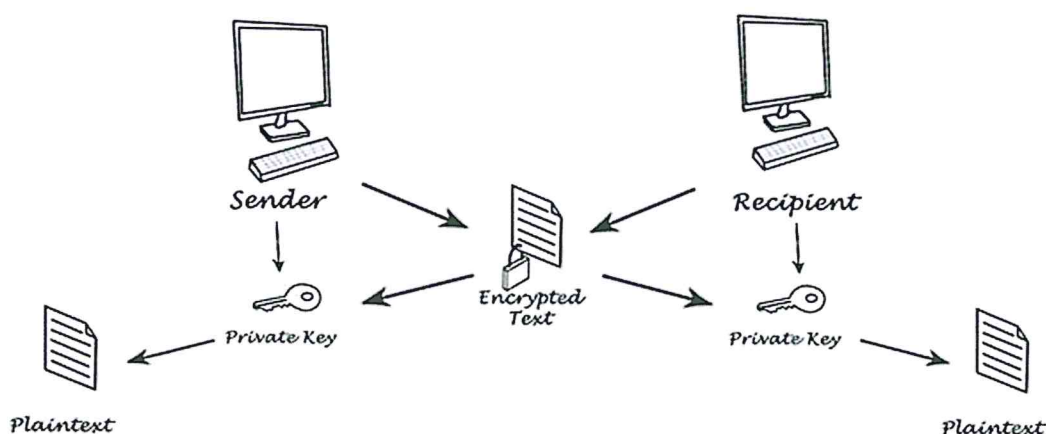


Figure 2.2: Symmetric Encryption

2.1.3 Asymmetric Encryption:

As a solution for the not completely safe Symmetric Encryption, there is the Asymmetric Encryption system that uses a pair of keys for added security: a private and a public key. The private key is for you and the public key is published online for others to see.

The public key is used to access the encryption code that corresponds to your private key. So, if you are sending an encrypted message to Susan which you do not want others to see, you would use her public key to encrypt it. She will be able to decrypt it with her own corresponding private key. Likewise, if she

sends a message to you, she uses your public key to encrypt the message and you would use your private key to decrypt it.

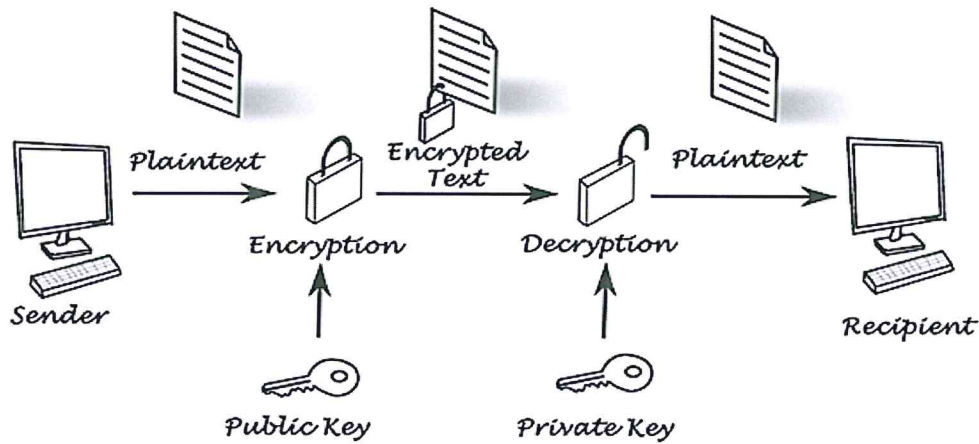


Figure 2.3: Asymmetric Encryption

The most popular public-key algorithm is The RSA

This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key, this makes the RSA algorithm a very popular choice in data encryption.

First of all, two large distinct prime numbers p and q must be generated. The product of these, we call n is a component of the public key. It must be large enough such that the numbers p and q cannot be extracted from it - 512 bits at least i.e. numbers greater than 10154. We then generate the encryption key e which must be co-prime to the number $m = \varphi(n) = (p - 1)(q - 1)$.

We then create the decryption key d such that $de \bmod m = 1$. We now have Both the public and private keys [3].

2.1.4 Monoalphabetic Substitution:

One simple example of symmetric key cryptography is the Monoalphabetic substitution. In this case, the relationship between a character in the plaintext and a character in the ciphertext is always one-to-one. An example Monoalphabetic substitution is the Caesar cipher. As shown in Fig.2.4, in this approach a character in the ciphertext is substituted by another character shifted by three places, e.g. A is substituted by D. Key feature of this approach is that it is very simple but the code can be attacked very easily [4].

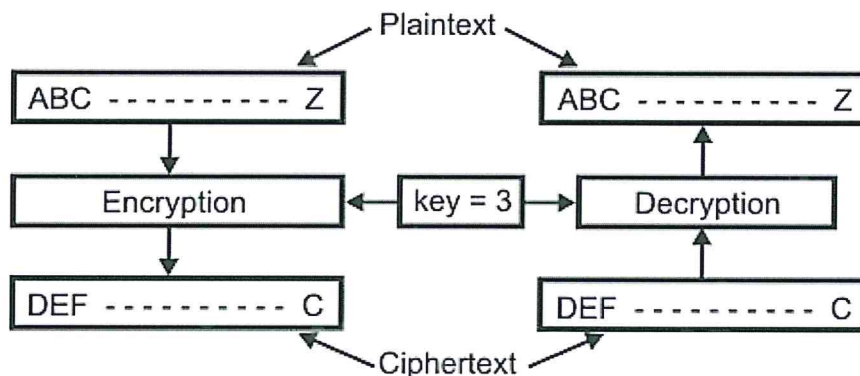


Figure 2.4: The Caesar cipher

2.1.5 Polyalphabetic Substitution:

This is an improvement over the Caesar cipher. Here the relationship between a character in the plaintext and a character in the ciphertext is always one-to-many. Example of polyalphabetic substitution is the Vigenere cipher [4].

2.1.6 Transpositional Cipher:

The transposition cipher, the characters remain unchanged but their positions are changed to create the ciphertext.

Transpositional cipher is also not a very secure approach. The attacker can find the plaintext by trial and error utilizing the idea of the frequency of occurrence of characters [4].

2.1.7 Cryptographic goals:

1. Confidentiality is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.

2. Data integrity is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

3. Authentication is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).

4. Non-repudiation is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another

entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.















2.2 Visual secret sharing scheme:

Appropriate techniques are required to prevent illicit usage of information. Such techniques are called as Secret Sharing Schemes. G.R. Blakley and Adi Shamir independently invented secret sharing scheme in 1979[5]. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image based secrets. Moni Naor and Adi Shamir proposed the basic model of visual cryptography [5]. The main concept of the original visual cryptography scheme is to encrypt a secret image into some shares. Secret information cannot be revealed with few shares. All shares are necessary to combine to reveal the secret image. There has been a steadily growing interest in visual cryptography. Visual cryptography is simple, secure and effective cryptographic scheme [6].

2.3 Black and White Visual Cryptography Schemes:

Naor and Shamir's [5]. proposed encoding scheme to share a binary image into two shares Share1 and Share2 . If pixel is white one of the above two rows of Table 2:1 is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows of Table 1 is chosen to generate Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed.

Table2:1. Naor and Shamir's scheme for encoding a binary pixel into two shares.

















Pixel	Probability	Share ₁	Share ₂	Share ₁ ⊗ Share ₂
	50%			
	50%			
	50%			
	50%			

2.4 (2, 2) Visual Cryptography Scheme:

In (2, 2) Visual Cryptography Scheme, original image is divided into 2 shares. Each pixel in original image is represented by non-overlapping block of 2 or 4 sub-pixels in each share. Anyone, having only one share will not be able to reveal any secret information. Both the shares are required to be superimposed to reveal the secret image [5]. There are many techniques for encoding the pixels of original image. In a technique, in which each pixel in original image is represented by two sub-pixels in each share, while reading the pixels in original image, if a white pixel is encountered, one of the first two rows in Table 2:2 is selected with probability 0.5, and the shares are assigned 2 pixel blocks as shown in the third and fourth columns in Table 2:2. Similarly, if a black pixel is encountered, one of the last two rows is selected with probability 0.5, from which a sub-pixel block is assigned to each share. When two shares are superimposed, if two white pixels overlap, the resultant pixel will be white and if a black pixel in one share overlaps with either a white or black pixel in another share, the resultant pixel will be black.

This implies that the superimposition of the shares represents the Boolean OR function. The last column in Table 2:2. shows the resulting sub-pixel when the sub-pixels of both the shares in the third and fourth columns are superimposed [5].

Table 2:2 (2 out of 2) using 2 subpixels per original pixel

Original Pixel	Probability	Share 1 Sub-Pixel	Share 2 Sub-Pixel	Share 1 Share 2
	0.5			
	0.5			
	0.5			
	0.5			

2.5 (k, n) Visual Cryptography Scheme:

In (2, 2) visual cryptography, both the shares are required to reveal secret information. If one share gets lost due to some technical problem, secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal information and user can not afford to lose a single share. To give some flexibility to user, basic model of visual cryptography proposed by Naor and Shamir can be generalized into a visual variant of k out of n visual cryptography scheme [5]. In (k, n) visual cryptography scheme, n shares can be generated from original image and distributed. Original image is recognizable only if k or more shares stacked together, where value of k is between 2 to n. If fewer than k shares stacked together, original image cannot be recognized. It gives flexibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained.

2.6 Visual Cryptography Scheme for General Access Structure:

In (k, n) visual cryptography scheme, all n shares have equal importance. Any k out of n shares can reveal the secret information. It may compromise the security of system. To overcome this problem, G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extended (k, n) visual cryptography model to general access structure [7]. In general access structure scheme, given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any k shares from qualified subset of shares can reveal secret information, but less than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can't reveal secret information so; Visual cryptography for general access structure improves the security of system

2.7 Visual Cryptography Scheme for Grey images:

All previous visual cryptography schemes were only limited to binary images. These techniques were capable of doing operations on only black and white pixels. It is not sufficient for real life applications. Chang-Chou Lin, Wen-Hsiang Tsai proposed visual cryptography for gray level images [8]. In this scheme a dithering technique is used to convert gray level image into approximate binary image.

Then existing visual cryptography schemes for binary images are applied to create the shares.

2.8 Visual Cryptography Scheme for Color images:

Visual cryptography schemes were applied to only black and white images till year 1997. Verheul and Van Tilborg proposed first color visual cryptography scheme [9]. In this visual cryptography scheme one pixel is distributed into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel,

there is exactly one color region colored, and all the other color regions are black.

F.Liu, C.K.Wu, X.J. Lin proposed a new approach for colored visual cryptography scheme [10]. They proposed three different approaches for color image representation:

1- In first approach, colors in the secret image can be printed on the shares directly. It works similar to basic visual cryptography model. Limitations of this approach are large pixel expansion and quality of decoded image is degraded.

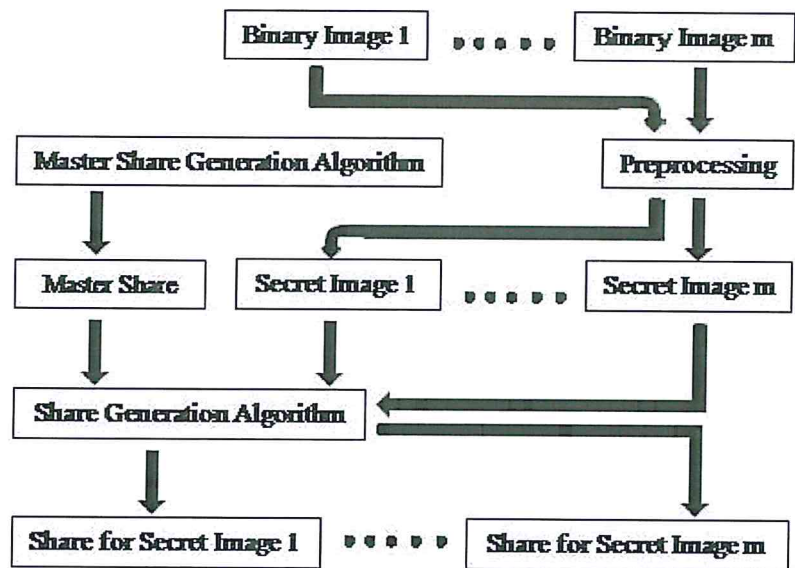
2- In second approach separate three color channels are used. Red, green, blue for additive model and cyan, magenta, yellow for subtractive model. Then normal visual cryptography scheme for black and white images is applied to each of the color channels. This approach reduces the pixel expansion but quality of image gets degraded due to halftoning process.

3- In third approach, binary representation of color of a pixel is used and secret image is encrypted at bit-level. This results in better quality of image.

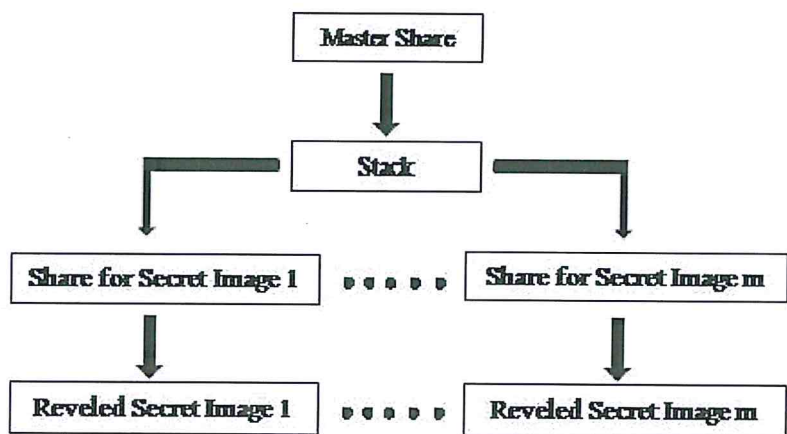
An extended visual cryptography (EVC) provide techniques to create meaningful shares instead of random shares of traditional visual cryptography and help to avoid the possible problems, which may arise by noise-like shares in traditional visual cryptography.

2.9 Related Works:

Mandal, J.K. and Ghatak, S. [11], In proposed a novel $(2, m + 1)$ visual cryptographic technique, where m number of secret images were encrypted based on a randomly generated master as a common share for all secrets which was decodable with any of the shares in conjunction with master share out of $m + 1$ generated shares. Instead of generating new pixels for share except the master share, hamming weight of the blocks of the secret images were been modified using random function to generate shares corresponding to the secrets. At the end of their work, the proposed scheme was secure and very easy to implement like other existing techniques of visual cryptography. At the decoding end the secrets were revealed by stacking the master share on any one share corresponding to the secrets in any arbitrary order with proper alignment directly by human visual system where shares were printed on different transparencies which conforms the optimality of using shares. The aspect ratio and dimension of the secret images and the generated shares with respect to the source images remained constant during the process.



(a)



(b)

Figure 2.5: Schematic diagram of SCOSVC algorithm (a) Encoding algorithm (b) Decoding algorithm

Shyamalendu Kandar , Arnab Maiti [12] They proposed a variable length Symmetric Key based Visual Cryptographic Scheme for color images where a secret key is used to encrypt the image and division of the encrypted image is done using Random Number. Unless the secret key, the original image will not be decrypted. Here secret key ensures the security of the scheme and visual cryptography is used to break the image into number of shares.

Overall process:

Step I: Any combination of characters [Characters, Numbers and Special Symbol] of any length is taken as KEY, which is XOR ed with the pixel array computed from the original image. This makes the image blur to some extent.

Step II: The encrypted image is divided into n number of shares using k-n secret sharing visual cryptography scheme such that k number of shares is sufficient to reconstruct the encrypted image.

Step III: k number of shares produced in Step II is stacked together to reconstruct the encrypted image.

Step IV: The KEY taken in Step I is XOR ed with the image produced in Step III, to generate the original image. This is described by the following figure:

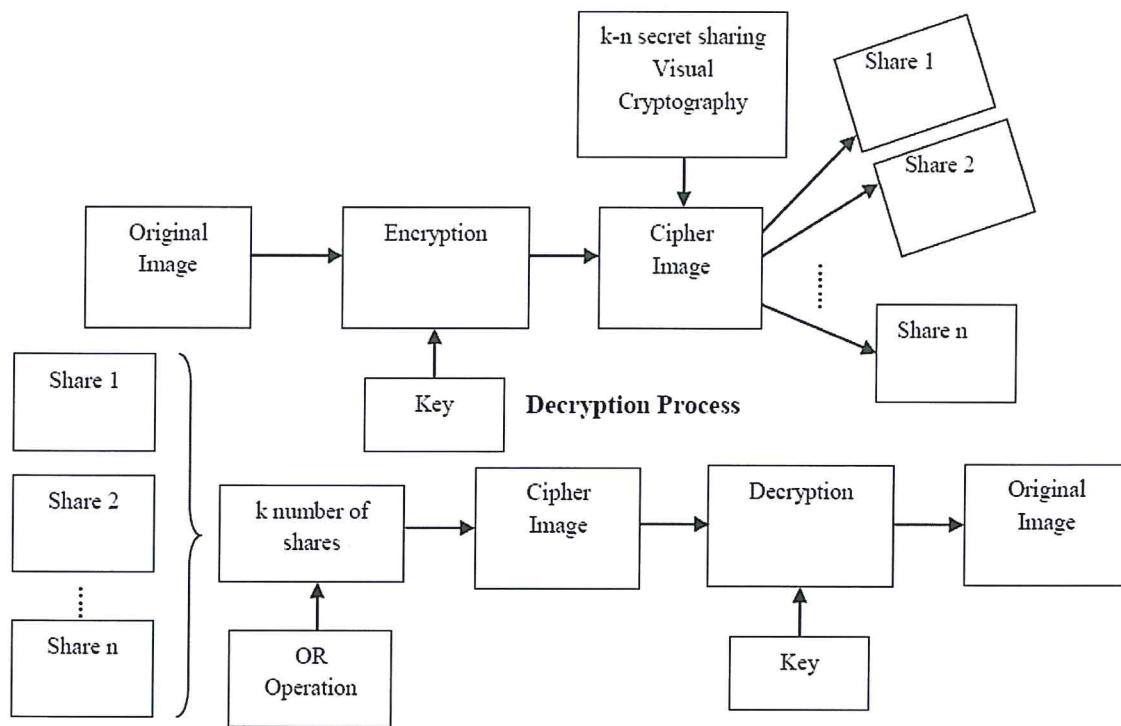


Figure 2.6: Block diagram of the overall procedure

Quist-Aphetsi Kester [13] developed a cipher algorithm for image encryption of $m*n$ size by shuffling the RGB pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel. The algorithm was implemented effectively without change in the image size and was no loss of image information after decryption.

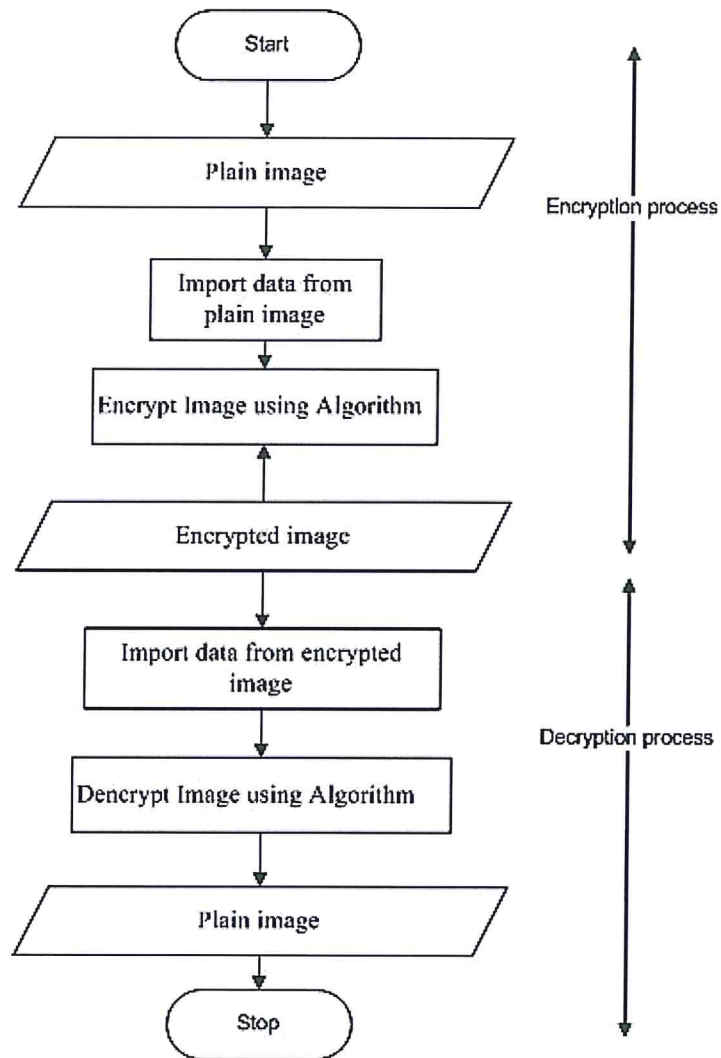


Figure 2.7: The flow chart diagram for the encryption and decryption process

Akhil Anjekar. et al [14] Variable length key based visual cryptography for color image uses a variable length Symmetric Key based Visual Cryptographic Scheme for color images where a secret key is used to encrypt the image and division of the encrypted image is done using Random Number. Unless the

secret key, the original image will not be decrypted. Here secret key ensures the security of image.

Image encryption using secret key: Original image is encrypted using key. A user generated any combination of characters of varying length gives a key. Generated key and original image are taken as input. Pixel array is computed from original image and key is XOR ed with pixel array to give encrypted image. The contents of original image and encrypted image are totally different, this process makes encrypted image blur to some extent and provide security.

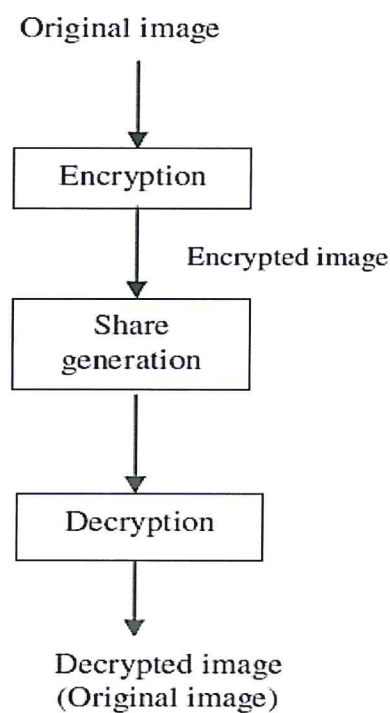


Figure 2.8 Overall process of (VLKBVCSCI)

Paper name	Most Important Features	Share generation process	Generated shares contain	Decryption is process
A Novel Technique for Secret Communication through Optimal Shares using Visual Cryptography (SCOSVC)	*less overheads than existing techniques * that for m secret communication only m + 1 shares are generated	numbers of shares are generated depending on the master share and m secret images	quality of the generated shares with respect to the image dimension and aspect ratio is constant	stacking the master share on any one share corresponding
Variable Length Key based Visual Cryptography Scheme for Color Image using Random Number	the key makes it more secure.	applied on encrypted image by key. Key encryption makes the Original image blur.	Generated shares have totally different contents.	Decryption is done by OR as well as XOR operation.
Image Encryption based on the RGB PIXEL Transposition and Shuffling	The extra swapping of RGB values in the image file after R G B component shifting has increased the security of the image	Applied on original image	there were no changes of the bit values of the images	Decryption is done by OR Operation
VARIABLE LENGTH KEY BASED VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGE	more secure using key	applied on encrypted image.	Generated shares content different from original image contents.	Decryption is done by OR as well as XOR with the key.

Table1 2.3: Related works comparison

CHAPTER 3
METHODOLOGY AND TOOLS

3.1 Overview:

Digital image are electronic snapshots taken of a scene or scanned from documents, such as photographs, manuscripts, printed texts, and artwork. The digital image is sampled and mapped as a grid of dots or picture elements (pixels). Each pixel is assigned a tonal value (black, white, shades of gray or color), which is represented in binary code (zeros and ones). The binary digits ("bits") for each pixel are stored in a sequence by a computer and often reduced to a mathematical representation (compressed). The bits are then interpreted and read by the computer to produce an analog version for display or printing [15].

3.2 Types of Digital image:

3.2.1 Binary images:

Are images whose pixels have only two possible intensity values. They are normally displayed as black and white [16].

3.2.2 Grayscale image:

Is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest [16].

3.2.3 Color images:

Are a digital image that includes color information for each pixel. are stored in either 24-bit (true color images) or 8-bit per pixel files. A common image size is 640×480 pixels and 256 colors (or 8 bits per pixel) Represent colors RGB [16].

3.3 Medical Image:

Is the technique and process of creating visual representations of the interior of a body for clinical analysis and medical intervention [19] have many kinds of them:

3.3.1 X Ray Image:

X rays image are electromagnetic radiation that differentially penetrates structures within the body and creates images of these structures on photographic film or a fluorescent screen. These images are called diagnostic x rays [19].

3.3.2 Magnetic resonance imaging (MRI):

is an imaging technique used primarily in medical settings to produce high quality images of the soft tissues of the human body [17].

3.4 Proposed Method:

For encryption , firstly, a secret key will be generated then a summation of the key with the original image will take place. Then, the key will be used to encrypt the plain image (the original image) using the function:

$$sk = \left[|(He - Pi)| + (a \times b) + \left| \left(\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i \right) \right| \right] \bmod a$$

After that, the encrypted image will be separated into three platters; that is to extract the RGB from that image. Each of which will be composed with the same bits and pixels of the original image but with one extracted color: first platter will produce the image with only the red ratio for all pixels from that image, the second one contains pixels with only blue ratio, and the third one contains just the green ratio of that pixels.

The generated key will be used then once again to encrypt each platter individually and separately from the other. And then each platter will get permuted; that is to exchange the locations of columns of pixels with the rows.

Finally, reshaping the resultant platters will be performed for each platter; the numerical values of the pixels for that platter are then displaced from their respective positions to arrive finally to what is called 'share'- the encrypted pattern.

In decryption process, the vice-versa of the whole operations that we performed earlier in the encryption will be done. The key is used to subtract the numeric values of the image instead of summation. Last step in decryption is that to stack the shares in order to get the original image. The processes are shown in figure 3.1: below.

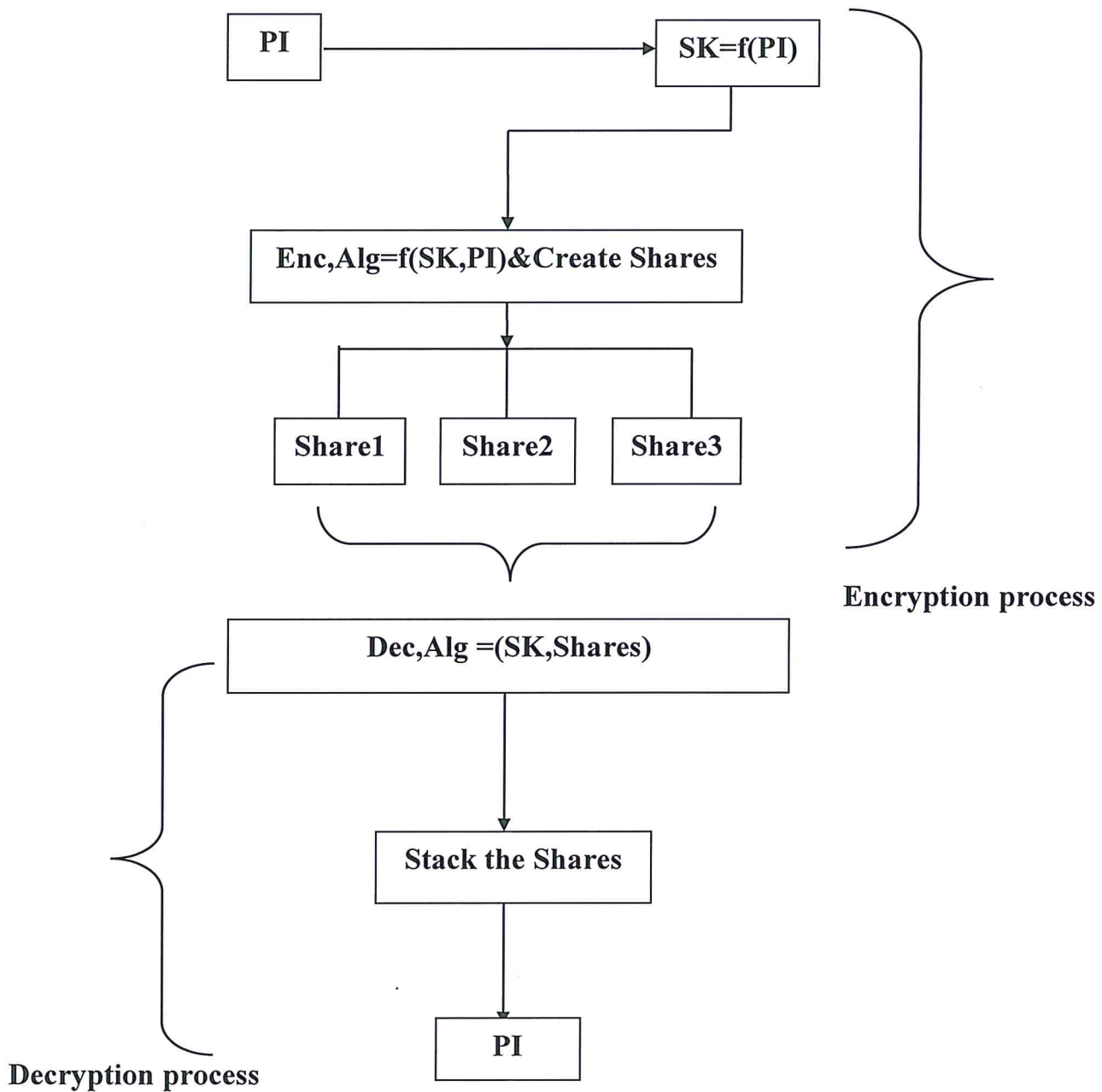


Figure 3.1: The encryption and the decryption process

In figure 3.1, PI is the plain image and Share1, Share 2 and Share3 is the ciphered image. Sk is the secret key used in the encryption and the decryption process of the image. Enc.Alg is the encryption algorithm and Dec.Alg is the decryption algorithm employed.

3.5 RGB colors shuffled Algorithm:

1. Start
2. Import data from image and create an image graphics object by interpreting each element in a matrix.
3. Get the size of r as [a, b]
4. Get the Entropy of the plain Image
5. Get the mean of the plain Image
6. Compute the shared secret from the image
7. Iterate step 8 to 13 using secret key value
8. Extract the red component as 'r'
9. Extract the green component as 'g'
10. Extract the blue component as 'b'
11. Let r =Transpose of r
12. Let g =Transpose of g
13. Let b =Transpose of b
14. Reshape r into (r, a, and b)
15. Reshape g into (g, a, and b)
16. Reshape b into (b, a, and b)
17. Finally the data will be converted into an image format to get the shares.

The secret key is obtained as follows:

$$sk = \left[|(He - Pi)| + (a \times b) + \left| \left(\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i \right) \right| \right] \bmod a$$

Where a, b are dimension of the image and He is the entropy value of the image and x bar is the arithmetic mean for all the pixels in the image.

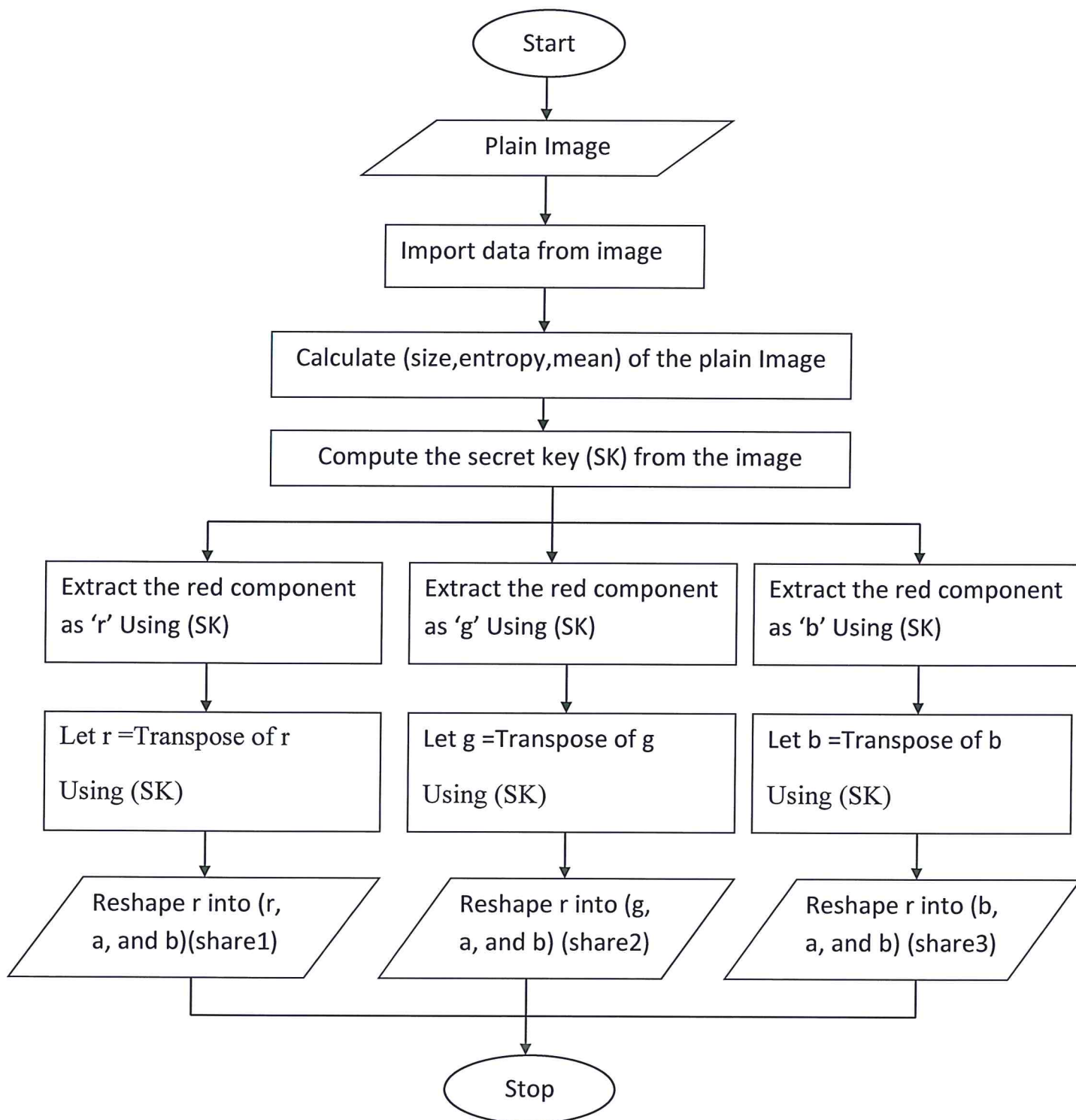


Figure 3.2: Flow chart for RGB Pixel-Shuffling Encryption and create share using secret key

3.6 Application and tools:

MATLAB is a "programming" application which allows its users to perform a variety of complex scientific calculations and graphical visualization.

or is a program that allows you to carry out computations in a straightforward manner, removing much of the tedium involved in programming. It is extremely useful for creating simulations of neural networks, as well as for general types of data analysis and visualization [18].

Advantages of Matlab:

- Ease of use
- Platform independence
- Predefined functions
- Matlab makes use of highly respected algorithms and hence you can be confident about your results.
- You can build up your own set of functions for a particular application.

Disadvantages of Matlab:

- Can be slow
- Expensive

CHAPTER 4
RESULTS AND DISCUSSION

4.1 Results:

The implantation of the algorithm was done using MATLAB Version 7.8.0 R2009a. The image sizes used were not fixed since the algorithm can work on $m \times n$ image size. The algorithm was written in m-file and tested on sample of medical images.

Three samples of medical images were encrypted by the algorithm using MATLAB and the results are below.

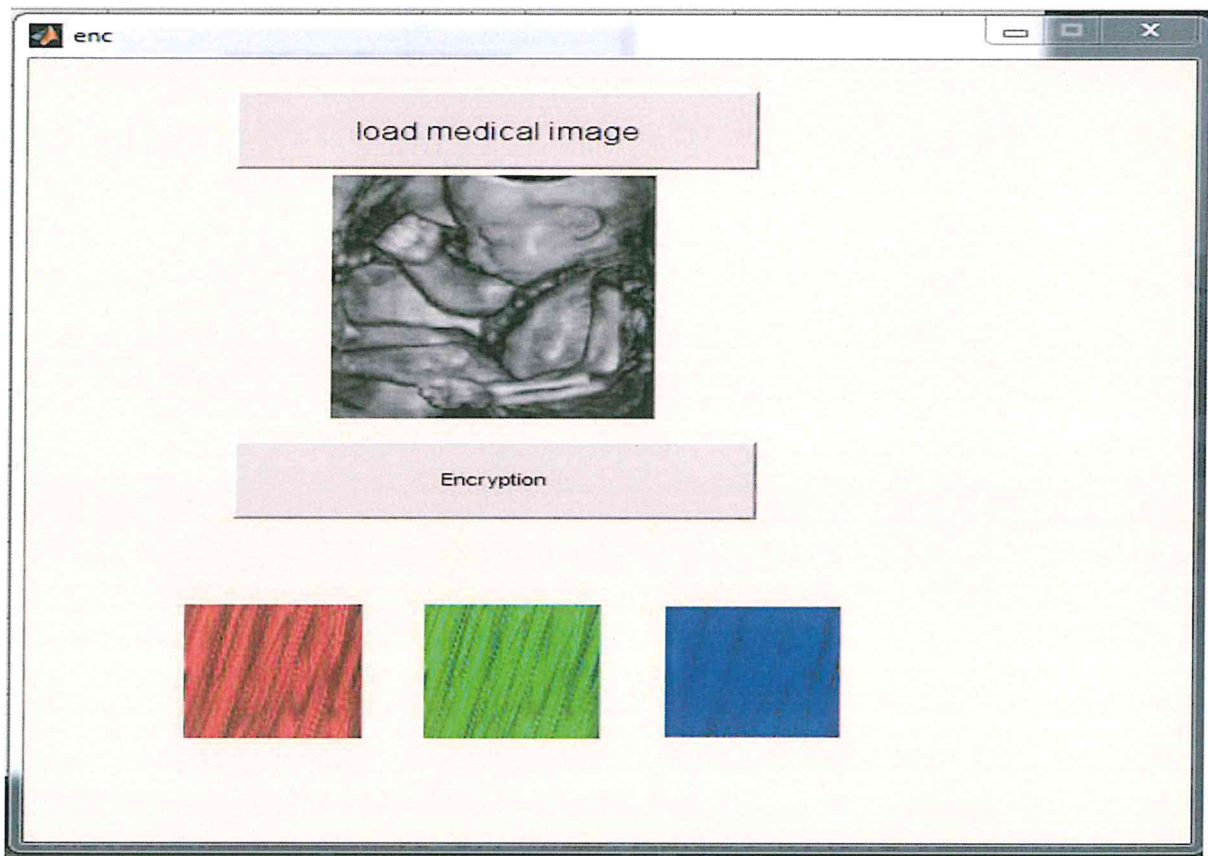


Figure 4.1: Graphical user interface for encryption process

The figure above illustrates the graphical user interface of executing the application to encrypt such images. Two buttons are found, the 'load image' which loads the image that the user aims to encrypt after clicking on it, and

‘encryption’ button which execute the steps of encryption algorithm we explained earlier in the preceding chapter , section 3.4

The image which is placed under the first button is the loaded, plain image. The three images under the second button are the resultant shares.

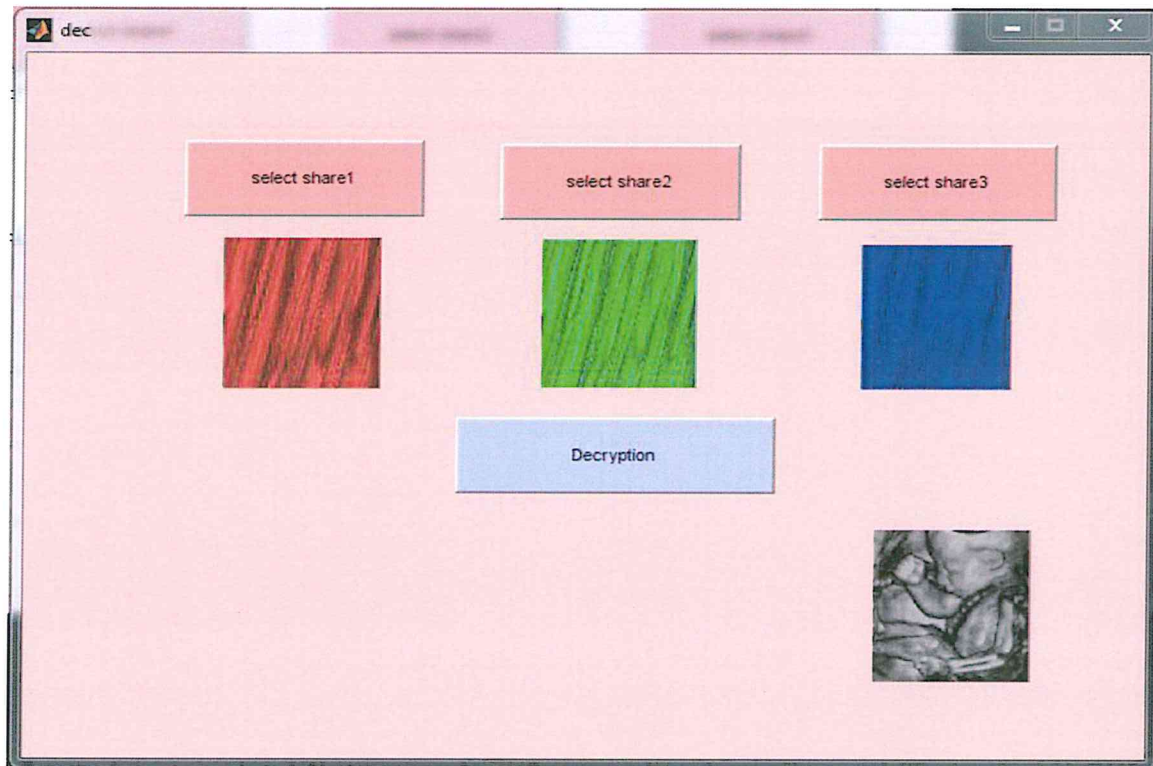


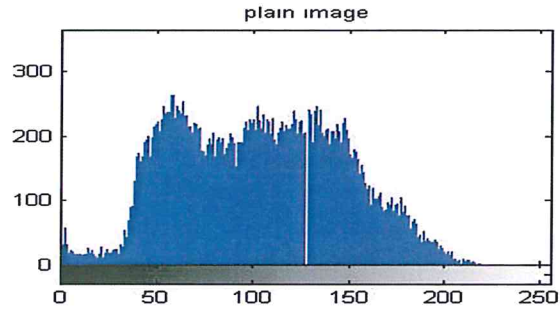
Figure 4.2: Graphical user interface for decryption process

DECRYPTION

The figure above illustrates the decryption process. Four buttons are available, namely, ‘select share1’, ‘select share2’, ‘select share3’, and ‘Decryption’. The three buttons above loads the three shares, then the 4th button performs the decryption process and stacking the shares into one image to produce finally the plain image.



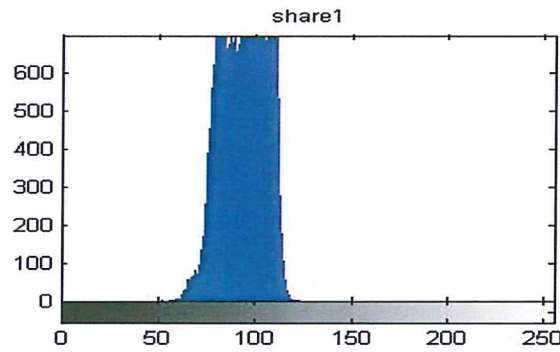
(a) Plain image



An RGB graph of figure 4.3 (a)



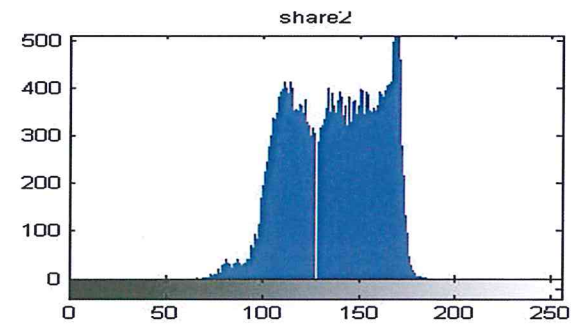
(b) Share1



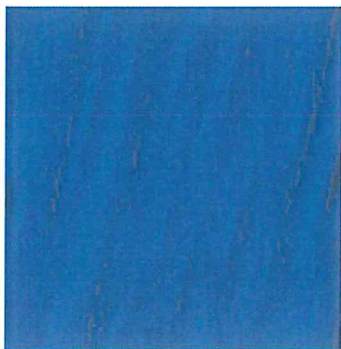
An RGB graph of figure 4.3 (b)



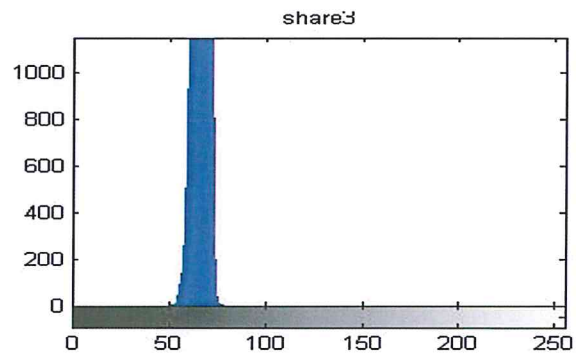
(c) Share2



An RGB graph of figure 4.3 (c)



(d) Share3

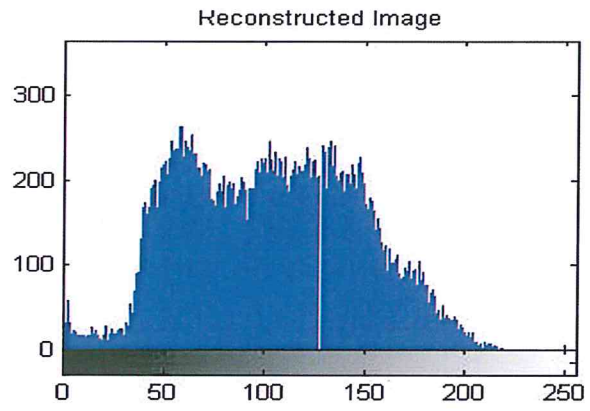


An RGB graph of figure 4.3 (d)

Figure 4.3: Encryption Ultra sonic Image of the womb

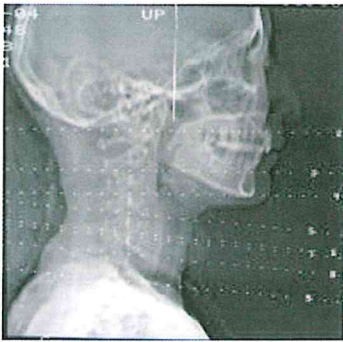


(a) Decrypt image

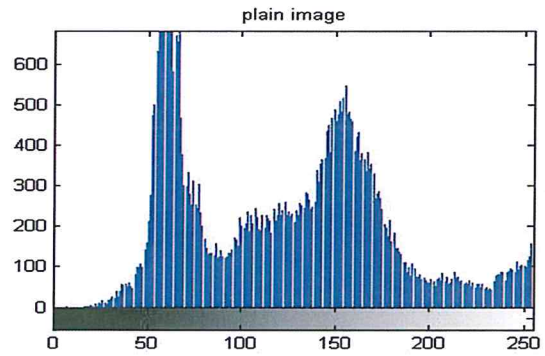


An RGB graph of figure 4.4 (a)

Figure 4.4: Decryption Ultra sonic Image of the womb



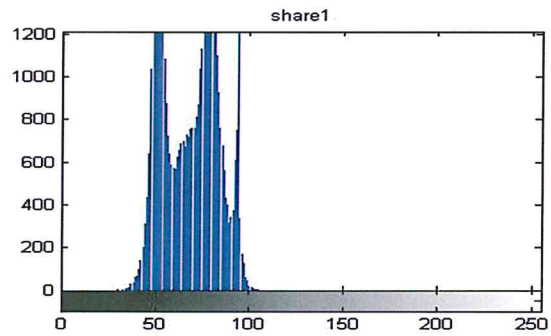
(a) Plain image



An RGB graph of figure 4.5 (a)



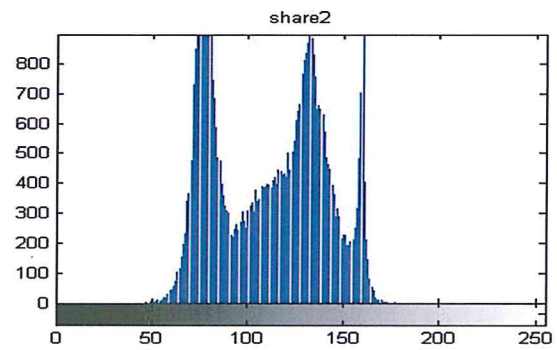
(b) Share 1



An RGB graph of figure 4.5 (b)



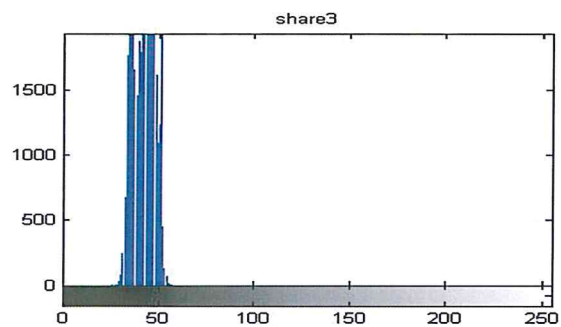
(c) Share 2



An RGB graph of figure 4.5 (c)

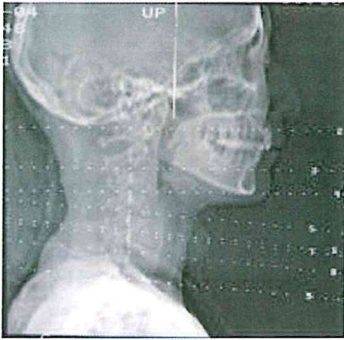


(d) Share 3

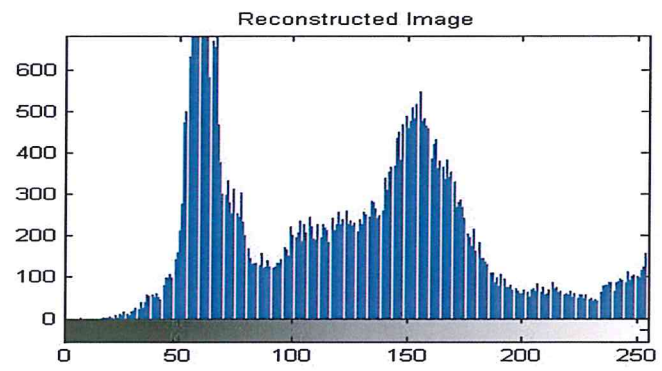


An RGB graph of figure 4.5 (d)

Figure 4.5: Encryption X-ray picture of the brain

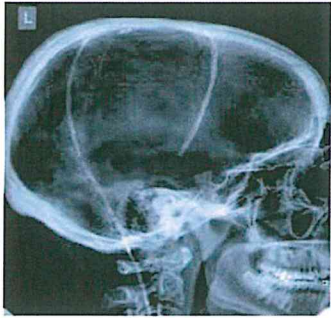


(a)Decryption image

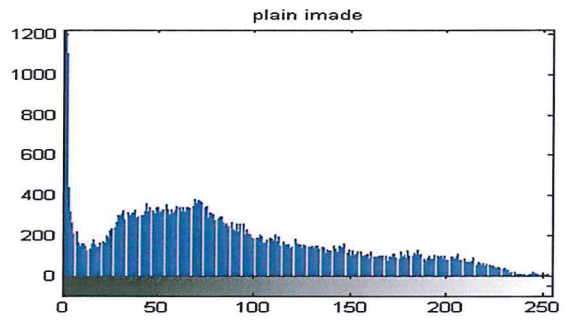


An RGB graph of figure 4.6 (a)

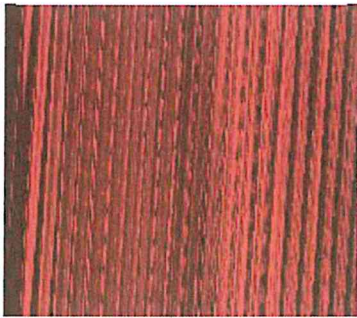
Figure 4.6: Decryption X-ray picture of the brain



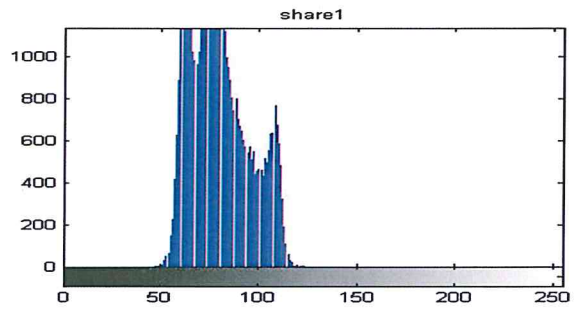
(a) Plain image



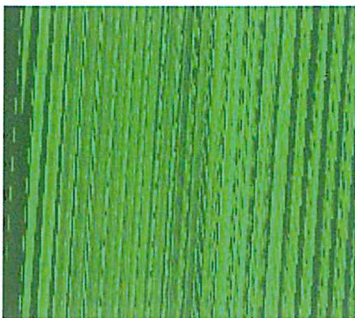
An RGB graph of figure 4.7 (a)



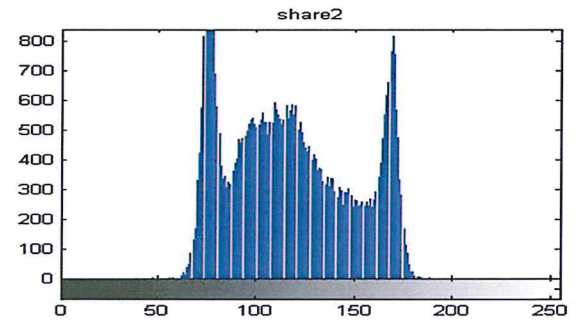
(b) Share 1



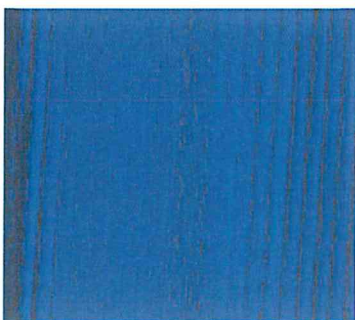
An RGB graph of figure 4.7 (b)



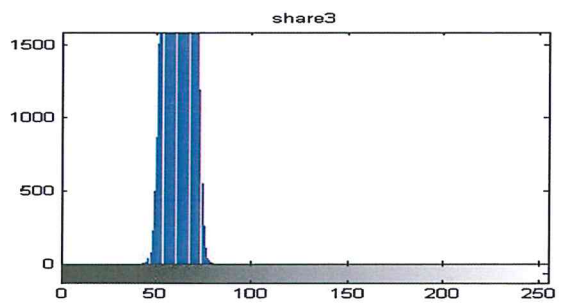
(c) Share 2



An RGB graph of figure 4.7 (c)



(d) Share 3

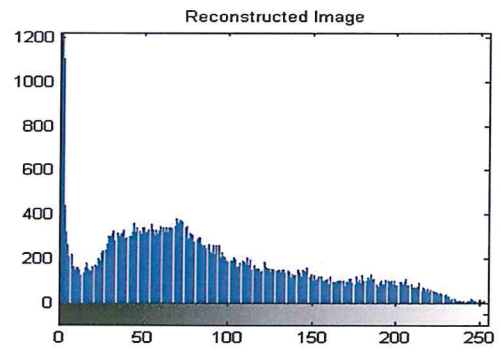


An RGB graph of figure 4.7 (d)

Figure 4.7: Encryption X-ray picture of the brain

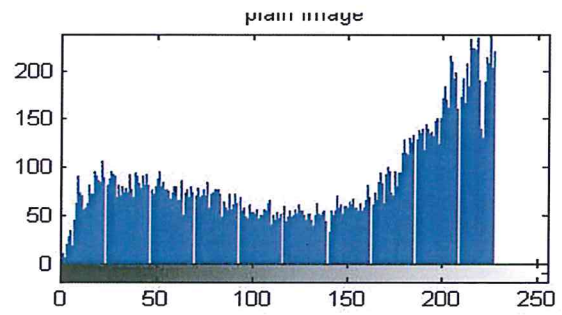
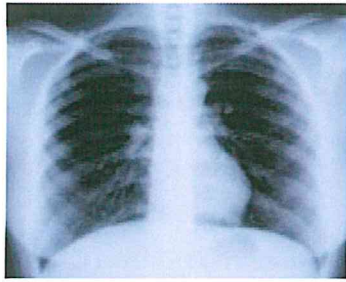


(a)Decryption image

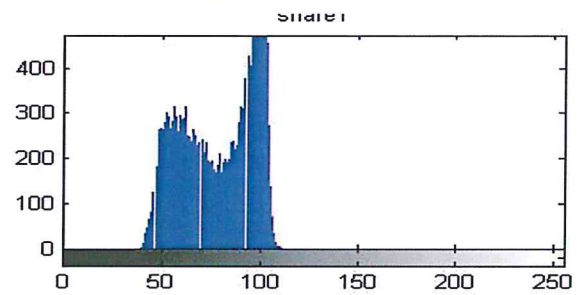
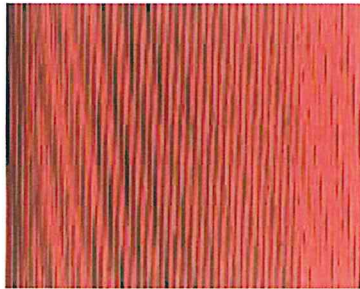


An RGB graph of figure 4.8 (a)

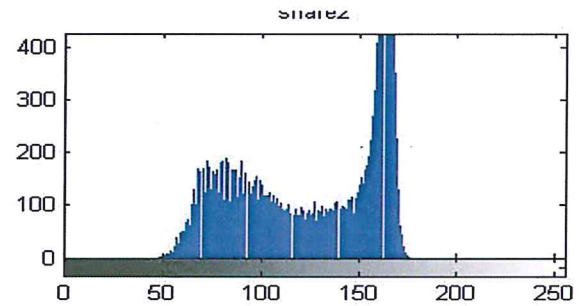
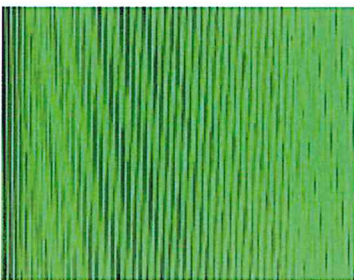
Figure 4.8: Decryption X-ray picture of the brain



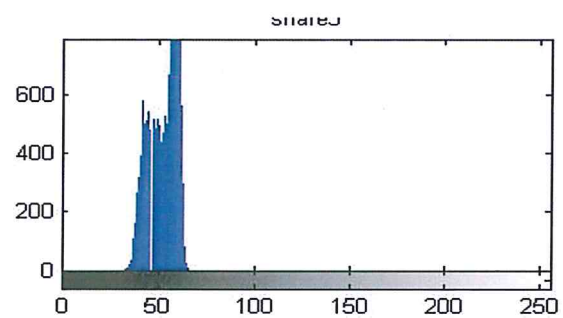
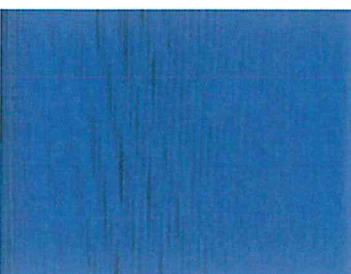
An RGB graph of figure 4.9 (a)



An RGB graph of figure 4.9 (b)



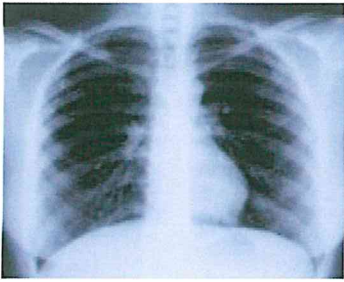
An RGB graph of figure 4.9 (c)



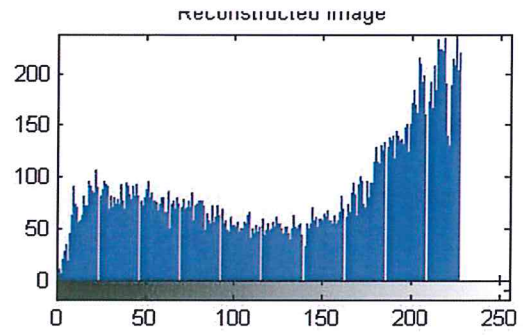
An RGB graph of figure 4.9 (d)

(d)Share 3

Figure 4.9: Encryption X-ray picture of the ribs



(a)Decryption image



An RGB graph of figure 4.10 (a)

Figure 4.10: Decryption X-ray picture of the ribs

4.2 Discussion:

In the encryption process, the images used had their RGB colors shuffled to obtain Shares.

The shares of the images for this research were dependent solely on the RGB pixel values of the images and the secret key obtained from the image.

The numerical values of the pixels were displaced from their respective positions and the RGB values were interchanged in order to obtain the ciphered images.

Secret shared key and visual cryptography are two distinct types of cryptography.

4.3 Statistical analysis:

To demonstrate that the proposed medical image encryption algorithm can resist statistical attack, tests have been done in terms of the entropy.

$$\text{Entropy} = \sum_i p_i \log_2 p_i$$

In the above expression, P_i is the probability that the difference between 2 adjacent pixels is equal to i , and \log_2 is the base 2 logarithms. for more details about the entropy of an image in [19].

The application of the proposed algorithm, we find that the average total pixel before encryption was the same as the average total pixel after encryption

The table below shows the entropy values for images in phase encryption and decryption.

Table 4.1: Entropy values of the plain image, cipher image and Reconstructed Image.

Image name	Plain ,cipher and decrypt image	Entropy value
Image1.jpg (Ultra sonic Image)	Plain image	7.3874
	Cipher image	7.4002
	Reconstructed Image	7.3874
Image2.jpg (X-ray picture)	Plain image	6.9587
	Cipher image	7.2999
	Reconstructed Image	6.9587
Image3.jpg	Plain image	7.4198
	Cipher image	7.4588
	Reconstructed Image	7.4198
Image4.jpg	Plain image	7.2923
	Cipher image	7.4952
	Reconstructed Image	7.2923

Entropy values for both plain image and the decrypted image (the reconstructed) should be the same; if the variance between them is 0 exact this is an indicator of the strength and high accuracy of the algorithm.

Table 4.2: comparisons with existing techniques

Other processes	Proposed scheme
Share generation process is applied directly on original image.[5] [20].	Share generation process is applied after Extract the RGB component.
Image size increasing [5].	During the process of encryption, the size of the image will remain as before.
Generated shares contain the original image contents [13].	Generated shares have totally different contents.
Do not provide more security.[11] [13].	Use of key makes it more secure.

CHAPTER 5
CONCLUSION AND RECOMMENDATION

5.1 Conclusion:

This proposed method makes it difficult for decrypting the image without prior knowledge of the algorithm and the secret key used. In this research the proposed method combines visual cryptography with shared secret key for the encryption and the decryption process.

The total entropy and the mean of the plain images never changed for all the ciphered images and the plain images. This makes the algorithm accurate and very effective for closely related images.

5.2 Recommendation:

This research shows how encryption algorithm provide security to medical imagery. The main objective is to guarantee the protection of medical images during transmission or store so it is recommend necessity applying security to the transmitted medical images to protect the privacy of patients.

It's also recommended that to use Public Key Infrastructure (PKI) instead of the generated keys we referred to in the methodology in chapter 3 above.

5.3 Future work:

This research has presented methods in order to protect the transmissions of medical images. Future researcher must focus on Compression techniques so as to reduce network bandwidth requirement of encrypted shares to reduce bandwidth requirement.

Reference:

1. Curry, I., *An Introduction to Cryptography and Digital Signatures*. Entrust Securing Digital Identities and Information, 2001.
2. Kester, Q.-A. and K.M. Koumadi. *Cryptographie technique for image encryption based on the RGB pixel displacement*. in *2012 IEEE 4th International Conference on Adaptive Science & Technology (ICAST)*. 2012.
3. Clark, B., *How does Encryption Work, and Is It Really Safe*. March 9 ,2015.
4. Kharagpur, *Network Security Module 8* CSE IIT.
5. Naor, M. and A. Shamir. *Visual cryptography*. in *Advances in Cryptology—EUROCRYPT'94*. 1995. Springer.
6. Bhagate, S.B. and P. Kulkarni, *An Overview Of Various Visual Cryptography Schemes*. International Journal of Advanced Research in Computer and Communication Engineering, 2013. **2**(9).
7. Ateniese, G., et al., *Visual cryptography for general access structures*. Information and Computation, 1996. **129**(2): p. 86-106.
8. Lin, C.-C. and W.-H. Tsai, *Visual cryptography for gray-level images by dithering techniques*. Pattern Recognition Letters, 2003. **24**(1): p. 349-358.
9. Verheul, E.R. and H.C. Van Tilborg, *Constructions and properties of k out of n visual secret sharing schemes*. Designs, Codes and Cryptography, 1997. **11**(2): p. 179-196.
10. Liu, F., C.K. Wu, and X.J. Lin, *Colour visual cryptography schemes*. Information Security, IET, 2008. **2**(4): p. 151-165.
11. Mandal, J. and S. Ghatak. *A Novel Technique for Secret Communication through Optimal Shares using Visual Cryptography (SCOSVC)*. in *Electronic System Design (ISED), 2011 International Symposium on*. 2011. IEEE.
12. Kandar, S. and A. Maiti, *Variable Length Key based Visual Cryptography Scheme for Color Image using Random Number*. International Journal of Computer Applications, 2011. **19**(4): p. 139-145.
13. Kester, Q.-A., *Image Encryption based on the RGB PIXEL Transposition and Shuffling*. International Journal of Computer Network and Information Security, 2013. **5**(7): p. 43.
14. Anjekar, A., P. Dahiwale, and S. Tarare, *VARIABLE LENGTH KEY BASED VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGE*.
15. <https://www.library.cornell.edu/preservation/tutorial/intro/intro-01.html>. 2000-2003
16. <http://homepages.inf.ed.ac.uk/rbf/HIPR2/binimage.htm>.
17. https://en.wikipedia.org/wiki/Medical_imaging.
18. Vitus, M., *An Introduction to MATLAB* January 13, 2007.

19. http://www.astro.cornell.edu/research/projects/compression/software2/entropy_func.pro.
20. SaiChandana, B. and S. Anuradha, *A new visual cryptography scheme for color images*. International Journal of Engineering Science and Technology, 2010. 2(6): p. 1997-2000.

الآية

قال تعالى: (قال الضيفُ عنده علمٌ من الكتابِ أنا أتيتك به قبل أن يرتك إليكَ طرفي فلما رآهُ مُحتقِرًا عندهُ قال هُنا من فضلِ ربِّي ليبتلوني أأخسرُ أم أُنقِرُ ومن خسرَ فإِنما يَخسرُ لِنَفْسِهِ ومن أنقِرَ فإنَّ ربِّي غنيٌّ كريمٌ صدقَ الله العظيم حوراء النمل الآية 40 .